U.S. Department of the Interior
Office of Inspector General

AUDIT REPORT

FOLLOWUP OF MAINFRAME COMPUTER POLICIES AND PROCEDURES, ADMINISTRATIVE SERVICE CENTER, BUREAU OF RECLAMATION

REPORT NO. 98-I-623
AUGUST 1998

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

AUG 20 1998

AUDIT REPORT

Memorandum

To: Commissioner, Bureau of Reclamation

From: Robert J. Williams
Assistant Inspector General for Audits

Subject: Audit Report on Follow-up of Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation (NO. 98-I-623)

INTRODUCTION

This report presents the results of our followup audit of recommendations contained in our March 1997 audit report "Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation" (No. 97-I-683). We performed this audit in support of audits of the annual financial statements of the Bureau of Reclamation and the Service Center's clients. Annual financial statements are required by the Chief Financial Officers Act. The objective of this audit was to determine whether (1) the Service Center had satisfactorily implemented the recommendations made in our prior audit report and whether any new recommendations were warranted and (2) the Service Center's general controls were effective over computer center management and operations, software change management, and mainframe computer operating system software.

BACKGROUND

The Bureau of Reclamation's Administrative Service Center in Denver, Colorado, is one of two Administrative Service Centers within the Department of the Interior. The Service Center's mission "is to improve economy and efficiency in Government through the delivery of standard. automated administrative systems." Specifically, the Service Center provides (1) consolidated payroll and personnel services for about 97,000 employees in the Department of the Interior and eight other Federal agencies and (2) Government accounting, integrated budgeting, and reporting services through the Federal Financial System (FFS) to three Departmental and five other Federal agencies. At the time of our audit. payroll and personnel services were provided through the Payroll/Personnel System (PAY/PERS) and the Federal Personnel Payroll System (FPPS) that was in the latter stages of development. The implementation of FPPS, which is to replace PAY/PERS, began in September 1997 with the conversion of three Departmental agencies from PAY/PERS. The remaining Departmental and non-Departmental agencies are to be converted to FPPS by December 30,

1998. In addition, a new client, the Social Security Administration, was added in March 1998, which increased the number of payroll accounts by about 65,000.

The Service Center provides its services on a cost-reimbursable basis, and this reimbursement function is administered through the Bureau's Working Capital Fund. The Service Center is organized into seven divisions that "provide data center, application, system, and operational support to the organization and clients" as follows:

- The ADP Services Division is responsible for (1) planning, developing, and operating the Service Center's computer center functions and (2) operating and maintaining computers, system software, and data communication networks. To assist the Division in carrying out its functions, the Service Center has contracted with Tri-Cor Industries, Inc. The Division provides data processing support for the Departmental standardized administrative sensitive systems.' To support these systems, the computer center operates an IBM mainframe computer using the "OS/390" operating system to manage the processing work load. The access control security software installed on the mainframe computer is the Resource Access Control Facility (RACF),[2] which controls users' and computer programs' access to the mainframe computer resources. Additionally, other system software, such as database management, telecommunications, and specialized vendor software, reside on the mainframe computer and are used to support the sensitive systems. Data center operations provide users with computer and communications equipment and infrastructure, systems software, and operational support. The Division manages data center operations through scheduling activities, planning for contingencies and capacity, and providing user support. The Division also manages the information resources security program.

- The FPPS Division is responsible for managing the development, implementation, and operation of the FPPS application. These responsibilities include controlling software changes; providing technical assistance to users; and managing tests of the application, converting data, and implementing the FPPS application. To assist the Division in carrying out its functions, the Service Center has contracted with the Computer Sciences Corporation.

- The Application Management Office directs the program activities of the Departmental administrative applications assigned to the Service Center.

- The PAY/PERS Division operates and maintains PAY/PERS. However, when all agencies have been converted to FPPS, the PAY/PERS Division will no longer exist.

'According to the National Institute of Standards and Technology, sensitive systems are defined as "systems that contain any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

[2]RACF is an IBM-licensed product that provides access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected accesses to protected resources, and logging detected unauthorized attempts to enter the system.

- The Payroll Operations Division plans, develops, executes, and manages the interagency payroll program delivered by the Service Center and performs payroll administration and services for all payroll clients.

- The Financial Systems Division provides functional and technical support to clients using FFS and related financial applications.

- The Management Services Division provides Service Center administrative support.

SCOPE OF AUDIT

The scope of our followup audit included an evaluation of the actions taken by Service Center management to implement the 24 recommendations made in our March 1997 audit report and a review of the general controls in place during fiscal year 1997. To accomplish our objective, we interviewed Service Center and contractor personnel, reviewed systems documentation, observed and became familiar with computer center operations, analyzed system security, reviewed system and application software maintenance procedures, and reviewed and tested implementation of the prior audit recommendations. Because our review was limited to evaluating the adequacy of internal controls at the Service Center, we did not test the effectiveness of the internal controls at the various agencies and clients supported by the Service Center.

Our audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Service Center's general controls over its mainframe computer and application systems that could adversely affect the data processing environment. The control weaknesses that we identified are summarized in the Results of Audit section and discussed further in Appendix 1 of this report. If implemented, our recommendations should improve the general controls in the areas cited. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the scope of this audit. However, the Office of Inspector General has issued two related reports as follows:

- The March 1994 audit report "Compliance With the Computer Security Act of 1987, Denver Administrative Service Center, Bureau of Reclamation" (No.94-I-3 57) stated that the Service Center generally complied with the requirements of the Computer Security Act of 1987 but that improvements were needed in the areas of security and operations. Since the Service Center was addressing all of the deficiencies identified, the report contained no recommendations.

- The March 1997 audit report "Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation" (No.97-I-683) stated that deficiencies identified in our March 1994 report relating to performing a risk analysis of the Service Center's local area networks and separating duties by using RACF security software still existed. This report contained 24 recommendations for improving management and internal controls at the Service Center. We reviewed actions taken by Service Center management to implement these recommendations as part of our current audit, the results of which are summarized in the Results of Audit section and discussed in Appendix 2 of this report.

RESULTS OF AUDIT

Regarding the prior report's recommendations, we found that the Bureau of Reclamation's Administrative Service Center management had satisfactorily implemented 21 of the 24 recommendations (see Appendix 2). Of the three remaining recommendations, one recommendation (No. D.3) was scheduled for completion by September 30, 1998, and we considered the planned actions adequate to correct the deficiencies identified. We considered the remaining two recommendations (Nos. G.2 and J.l) partially implemented because actions had not been completed to fully correct the previously identified deficiencies. The actions taken to implement the 2 1 recommendations have improved the controls in the areas of local area network protection; application access; mainframe system physical and logical security; and contingency planning, backup, and disaster recovery.

Regarding the general controls, we believe that overall, the general controls were operating with no material weaknesses. However, we found general control weaknesses in the areas of computer center management and operations, software change management, and mainframe computer operating system software that were present during fiscal year 1997. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," which defines minimal sets of controls for managing Federal information resources, and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies. Additionally, the Congress has enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls is adequate. Also, the Departmental Manual outlines (1) the requirements related to security clearance programs, suitability, and types of security investigations and (2) the process for determining position sensitivity. However,

Service Center management did not ensure that controls were implemented and were operating effectively and in compliance with established criteria. Specifically, we found that general control practices and processes were not complied with, the appropriate security levels were not assigned to automated data processing (ADP)-related positions, some mainframe computer functions were not operated efficiently, software change management controls were not complied with, and mainframe computer operating system software tools and settings had not been implemented to ensure system and data integrity. As a result, there was an increased risk of unauthorized access to, modification of, and disclosure of client-sensitive data; inefficient Service Center operations; and loss of system and data integrity.

Overall, we identified 6 weaknesses and made 14 recommendations for improving the general controls at the Service Center. The weaknesses in the areas of computer center management and operations, software change management controls, and mainframe computer operating system software are discussed in the following paragraphs, and details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Computer Center Management and Operations

We found that Government and contractor employees who filled ADP-related sensitive and critical positions did not have proper background clearances. Without information on the security-related background of personnel assigned to sensitive and critical positions, there was an increased risk that sensitive systems could be impaired or compromised. In addition, Service Center operations could be improved if some mainframe computer functions, such as moving changed software from the test environment to the production environment process and scheduling computer production, were centralized, and a standardized software change control tool was used. When mainframe computer functions are decentralized and not standardized, there is an increased risk of inefficient operations and unnecessary costs. We made three recommendations to address these weaknesses.

Software Change Management Controls

We found control weaknesses in the area of managing software changes made to the FPPS application and to the mainframe computer operating system. Because of the weak controls, there was an increased risk that unauthorized changes could be made to the sensitive FPPS application and to the critical operating system, which could affect application and system integrity. We made seven recommendations to address these weaknesses.

Mainframe Computer Operating System Software

We found that the Service Center had not implemented the available operating system software tools which would improve (1) the effectiveness of access controls to the mainframe computer resources and (2) mainframe computer system processing and data integrity. As a result, the risk was increased that access controls could be bypassed and unauthorized

activities would not be detected. We made four recommendations to address the weaknesses in this area.

Bureau of Reclamation Response and Office of Inspector General Reply

In the June 17, 1998, response (Appendix 3) to the draft report from the Commissioner, Bureau of Reclamation, the Bureau concurred with all 14 of the new recommendations. Based on the response, we consider Recommendations C. 1 and C.2 resolved and implemented and Recommendations A. 1, A.2, B. 1, C.3, D. 1, D.2, D.3, D.4, E. 1, E.2, F. 1, and F.2 resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

In its response, the Bureau said that "the report language regarding the FPPS system did not adequately consider that FPPS was under development during the time of the audit." We disagree. We clearly identified in Finding C that the weaknesses occurred during the latter stages of development and the early stages of implementation. However, we have added wording (page 1) to further clarify that the FPPS was in the latter stages of development during the period of our review.

Regarding our March 1997 report, we consider 2 1 recommendations resolved and implemented and the remaining 3 recommendations (Nos. D.3, G.2, and J.1) partially implemented. Accordingly, updated information on the status of the three prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Since the recommendations contained in this report are considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: In our prior report, we recommended that Service Center management require all contractor employees to have proper background clearances. However, during our current audit, we found that contractor personnel at the ADP Services Division had received background clearances but that not all contractor personnel at the FPPS and Financial Systems Divisions had received background clearances. Additionally, Service Center Federal personnel involved in designing, developing, operating, or maintaining sensitive automated systems did not have background checks and security clearances commensurate with their job responsibilities and the sensitivity of the information accessed. Specifically, 154 of the 189 Service Center employees who performed these ADP-related duties did not have the appropriate ADP background clearances.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," requires agencies to establish and manage security policies, standards, and procedures that include requirements for screening individuals participating in the design, development, operation, or maintenance of sensitive applications or those having access to sensitive data. In addition, the Departmental Manual (441 DM 4.6) requires position sensitivity levels of "non-critical sensitive" or "critical sensitive" and associated security clearances for ADP-related positions for which employees are required to design, test, operate, and maintain sensitive computer systems. Security clearances are also required of employees who have access to or process sensitive data requiring protection under the Privacy Act of 1974. Further, the Departmental Manual (441 DM 5.15) requires that all consultants or contractors performing ADP-related sensitive and critical duties have background investigations to determine position suitability and to receive a security clearance.

Cause: Service Center management had not uniformly developed and implemented, across all Service Center Divisions, personnel security policies requiring contractor personnel who perform ADP-related sensitive and critical duties to

COMPUTER CENTER MANAGEMENT AND OPERATIONS

be screened for position suitability. Additionally, Service Center management did not ensure that the level of position sensitivity for ADP-related positions was assigned at the level commensurate with the risk and sensitivity of the data accessed and processed and that background checks were performed on employees who filled these positions.

Effect: Without proper personnel background investigations, managers had limited knowledge of the suitability of their employees and contractors, from a security standpoint, for their respective jobs. Without this assurance, there was an increased risk that the Service Center's sensitive systems could be impaired or compromised by personnel.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Develop and implement policies and procedures which require contractor employees who fill ADP-related sensitive or critical positions to have documented suitability screening and proper background investigations and appropriate security clearances.

2. Evaluate the position sensitivity of ADP-related positions, assign position sensitivity levels in accordance with the Departmental Manual, and ensure that those employees working on sensitive systems have the proper background investigations and security clearances before they are assigned to the positions.

COMPUTER CENTER MANAGEMENT AND OPERATIONS

B. Operating Efficiencies

Condition: At the Service Center, each division controlled the process of moving changed software from the test to the production environment, different software tools were used to control the movement of the changed software, and internal and external clients controlled their mainframe computer production scheduling.

Criteria: Office of Management and Budget Circular A-l 30 states that management should oversee its processes to maximize return on investment and minimize financial and operational risk. Further, the Circular requires that financial management systems conform to the requirements of Office of Management and Budget Circular A- 127, "Financial Management Systems." Circular A- 127 requires that agency financial management systems process financial events effectively and efficiently.

Cause: Service Center management did not ensure that its processes were operating efficiently because of preferences of internal and external clients and because management had not developed and implemented consistent standards for controlling operational processes.

Effect: There was an increased risk that changed software would negatively impact the mainframe computer operating system; costs of maintaining different software tools would increase Service Center operating costs, which would be passed on to clients; and mainframe computer usage could be reduced. Additionally, without centralized control of production scheduling, there was an increased risk that critical processing jobs would not receive the required priority.

Recommendation:

We recommend that the Director, Administrative Service Center, in coordination with the Service Center's internal and external clients, evaluate the feasibility of centralizing the process of moving changed software from the test environment to the production environment, using standardized software tools to control the software change process, and centralizing mainframe computer production scheduling.

COMPUTER CENTER MANAGEMENT AND OPERATIONS

C. Application Software Change Management Controls

Condition: **Software** changes made to the FPPS during the latter stages of development and the early stages of implementation were not approved, reviewed, or evaluated adequately before changed software was installed for use in production; documentation was not adequate to monitor changes made to the software; and available library control software' was not implemented to ensure consistency and completeness throughout the FPPS application.

Criteria: Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," provides guidelines for managing software maintenance. Publication 106 states that all software changes should be carefully evaluated and formally reviewed prior to installing the changed software. The publication further states, "In order to monitor maintenance effectively, all activities must be documented. ... The key to successful documentation is that not only must the necessary information be recorded, it must be easily and quickly retrievable by the maintainer." In addition, FPPS Division policies and procedures require that all changes to the FPPS application be thoroughly documented, be accepted by all involved parties, and pass a quality assurance review.

Cause: FPPS Division management did not ensure that Division personnel followed software change management practices for making software changes to the FPPS application because of the time constraints to implement FPPS and because FPPS was encountering problems and was considered by Division personnel to be unstable. In addition, we found that FPPS Division management did not hold its personnel accountable for complying with Division policies and procedures when they made changes to the FPPS application. Further, FPPS Division management said that they did not implement the available library control software, which would ensure adequate documentation of the FPPS application, because at that time, the vendor library control software was not working correctly.

Effect: There was an increased risk that the changes made to the FPPS application would not perform according to specifications, which could adversely affect user satisfaction and could adversely impact other applications interfacing with the FPPS application or the mainframe operating system.

'Library control software is a system for keeping track of changes to and versions of software programs, documenting components to build executable programs, and preventing unauthorized access to program files.

COMPUTER CENTER MANAGEMENT AND OPERATIONS

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Require that software changes be adequately reviewed and approved before the changes are implemented.

2. Implement procedures to ensure that all software changes to the FPPS application are properly documented.

3. Implement the available library control software when corrected to ensure adequate documentation of the FPPS application.

COMPUTER CENTER MANAGEMENT AND OPERATIONS

D. Operating System Software Change Management

Condition: Change controls over the mainframe computer operating system software were not adequate. The ADP Services Division change control procedures did not address adequate separation of duties between the development, test, and installation functions. Thus, one individual could perform all of these critical functions. In addition, the change control procedures did not ensure that all changes were properly approved by Division management. While the change management procedures required approval of all software changes, changes were made without documented evidence of approval.

Criteria: Appendix III of Office of Management and Budget Circular A-l 30 states that one of the minimum controls required in a general support system is personnel controls. One such control is separation of duties, which is "the practice of dividing the steps in a critical function among different individuals." Also, Federal Information Processing Standards Publication 106 states that "to be effective, the policy should be consistently applied and must be supported and promulgated by upper management to the extent that it establishes an organizational commitment to software maintenance." In addition, Publication 106 states that "prior to installation, each change (correction, update, or enhancement) to a system should be formally reviewed." Finally, Division system change request procedures require that all change requests be approved by the appropriate branch chief.

Cause: ADP Services Division management did not ensure that appropriate separation of duties existed in developing and testing mainframe operating system software and parameter changes and in moving operating system software and parameter changes into the production environment, although the number of employees within the Division may allow for a separation of these duties. Additionally, Division management had not implemented controls to ensure that the process of making system software changes was in compliance with its documented procedures. Further, management had not implemented procedures to require periodic reviews of critical datasets and system parameters to identify inappropriate changes to the mainframe operating system environment. Although Division management had implemented a change control software tool that provided a systematic and automated means of controlling the movement of software changes, all the capabilities of the software tool were not implemented because of other Division priorities.

COMPUTER CENTER MANAGEMENT AND OPERATIONS

Effect: There was an increased risk that unauthorized, untested, and undocumented changes could be made to the mainframe computer operating system software and parameters, which would affect system processing and data integrity, and that these changes would not be detected or detected in a timely manner.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate current ADP Services Division procedures and determine the feasibility of implementing controls in the change management process over operating system software to ensure that adequate separation of duties is addressed and complied with.

2. Develop procedures and implement controls to ensure that changes to the operating system parameters are identified, approved by ADP Services Division management, and documented.

3. Develop procedures requiring periodic reviews of critical datasets and system parameters.

4. Evaluate implementing available capabilities in the current change control software tool to more effectively control changes to the operating system software.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

E. System Audit Tools

Condition: Service Center management did not use available mainframe computer operating system audit tools that would improve integrity over system processing and data and that would detect inappropriate actions by authorized users. Specifically:

- Operating system integrity verification and audit software was not used. Such software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures that may result from system setting options; from installing "back doors" to the operating system; and from introducing viruses and Trojan horses, which can destroy production dependability and circumvent existing security measures.

- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. System options that would log the results in the SYSLOG[2] of actions taken by the computer operators and system programmers affecting mainframe operating system configuration were not implemented. Therefore, an audit trail of the system initialization process and changes to the operating system configuration could not be produced for periodic review. Based on recommendations made by our audit staff during the review, Service Center management implemented the logging capabilities within the system; however, procedures had not been developed and implemented to require periodic reviews of the logs.

- Periodic reviews of critical System Management Facility (SMF)[3] logs to identify unauthorized changes to data by authorized users and critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as SET TIME, SET DATE, and SET SMF, all of which affect system processing and audit trails.

---

[2]SY SLOG is an audit trail that logs the results of actions taken by computer operators and system programmers during system initialization.

[3]The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identifying users who performed the activity.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

Criteria: Appendix III of Office of Management and Budget Circular A-l 30 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability includes reviewing or looking at patterns of users' behavior, which requires periodic reviews of the audit trails. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that audit trails are "technical mechanisms" to achieve individual accountability.

Cause: Service Center management did not acquire operating system integrity and verification software, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of available system logs. Instead, Service Center management relied on its staff to make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect: As a result, there was an increased risk that mainframe computer operating system security exposures would not be identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or detected timely and that the responsible individuals would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate acquiring system verification and auditing software.

2. Develop and implement procedures to ensure that periodic reviews are performed of the SYSLOG and critical SMF logs to identify unauthorized or inappropriate activities and that unauthorized or inappropriate activities are reported to Service Center management.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

F. Mainframe Operating System Options

Condition: ADP Services Division management did not implement mainframe operating system options that would strengthen controls over computer programs which access sensitive operating system functions. We found 13 libraries[4] that were able to run in the "Authorized Program Facility (APF)-authorized" state, even though the libraries were not required to run in the APF. By running in the APF-authorized state, these libraries may be considered part of the main&me operating system and thus have access to all of the mainframe resources.

Criteria: IBM's publication titled "OS/390 Initialization and Tuning Reference" states that "the parameter LNKAUTH specifies whether all libraries" in the LNKLST** member? "are to be treated as Authorized Program Facility (APF)-authorized when accessed as part of the concatenation, or whether only those libraries that are named in the APF table are to be treated as APF-authorized? Additionally, the publication addresses managing system security and states that the "authorized program facility (APF) allows your installation to identify system or user programs that can use sensitive system functions."

Cause: Division Management implemented a default option (LNKLST) that allowed libraries within the LNKLST** member to run in the APF-authorized state. An alternative option (APFTAB) is provided which requires only those libraries that are named specifically in the APF table to be able to run in the APF-authorized state. The 13 libraries were automatically added to the LNKLST** member when the operating system was upgraded in July 1997. Because Division management did not review the members used to define APF-authorized libraries, these 13 libraries remained in the LNKLST** member.

---

[4] A library is a collection of programs or data files or a collection of functions (subroutines) that are linked into the main program when it is compiled. (The Computer Language Company, Inc., Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

'Concatenation means to link together in a series or chain. (Webster's Ninth New Collegiate Dictionary, Merriam-Webster Inc., Springfield, Massachusetts, 1989, p. 27 1.)

[6] LNKLST** member "defines the collection of program libraries to be searched, in sequence, for programs when no specific [library] has been supplied in the job stream." (Mark S. Hahn, CONSUL Risk Management, Inc., A Guide to SYS1 .PARMLIB, Monograph Series 4, The Information Systems Audit and Control Foundation, Inc., Rolling Meadows, Illinois, February 1996, p. 38.)

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

Further, because Division management implemented the LNKLST option, these 13 libraries were unnecessarily provided the ability to run in the APF-authorized state. Therefore, management did not have assurance that only approved libraries had access to sensitive operating system functions. Based on recommendations of our audit staff during the review, the libraries were removed from the LNKLST** member. However, if the APFTAB option had been used, Division personnel would have been required to enter the 13 library names into the APF table, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Effect: By implementing the LNKLST option rather than the APFTAB option, the risk increased for unauthorized libraries to run in an authorized state, thus bypassing operating system controls, and for system integrity to be lost.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate the feasibility of using the APFTAB option, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

2. Perform periodic reviews of all members used to define the APF-authorized libraries to ensure that only those required to run in the APF-authorized state are given this authority.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "MAINFRAME COMPUTER POLICIES AND PROCEDURES, DENVER ADMINISTRATIVE SERVICE CENTER, BUREAU OF RECLAMATION" (No. 97-I-683)

Recommendations	Status of Recommendations and Corrective Actions
A. 1. Require all contractor employees to have proper background clearances.	Implemented. All contractor employees in the ADP Services Division are required to have background clearances. However, the current review found that contractor employees in other Service Center Divisions did not have appropriate clearances.
B.l. Enhance the intruder detection settings to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset.	Implemented. NetWare intruder lockout settings have been modified on all production servers to suspend a user identification (ID) for a period of 24 hours after three incorrect log-in attempts have been made within a 24-hour period.
Cl. Develop and periodically update a disaster recovery plan for the LAN.	Implemented. Subsequent to the completion of current fieldwork, the LAN Disaster recovery Plan was completed.
D.l. Ensure that LAN security and password features are implemented which will require all users to change passwords every 90 days; enforce unique password use; and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an as-needed basis.	Implemented. The password change interval has been revised to 90 days or less on all servers. Unique passwords are required for all individual users. Concurrent multiple connection authority has been removed from all accounts except for those where a demonstrated need exists.
D.2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.	Implemented. A procedure to secure the console on all Service Center file servers was implemented. At the monitor console screen, the "LOCK FILE SERVER CONSOLE OPTION" was implemented to lock the system console manually whenever the server is initialized.

Recommendations	Status of Recommendations and Corrective Actions
D.3. Ensure that the command "SET ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.	Partially implemented. All Service Center NetWare servers will be configured to require encrypted passwords when all Service Center NetWare file servers have been migrated to NetWare Directory Services. This is 75 percent implemented. The target date for full implementation originally was March 31, 1998, but the date has been changed to September 30, 1998.
E.l. Coordinate with the client to limit Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.	Implemented. As requested by the Service Center, the client has changed FFS security so that no employee has access to both vendor tables and disbursement documents.
F. 1. Document procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.	Implemented. Procedures for the issuance of card keys for vendors, contractors, and Federal employees have been documented.
F.2. Evaluate the need for individuals outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.	Implemented. The evaluation has been completed. Permanent card keys are issued to only those individuals deemed appropriate.

Recommendations	Status of Recommendations and Corrective Actions
F.3. Document procedures to ensure the Service Center's compliance with the Department of the Interior Automated Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.	Implemented. Procedures for monitoring visitor access to the computer room have been documented in compliance with the Departmental Handbook.
G. 1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau's Security Administrator.	Implemented. Evaluation of using one numeric or special character as part of the Service Center standard password has been completed. Service Center management, in coordination with its clients, determined that requiring numeric or special characters as part of the password was not feasible.
G.2. Reevaluate the standard RACF password change intervals and revocation settings to ensure that the level of risk associated with the mainframe applications and the current password settings is acceptable to the Service Center, as well as to its clients and the Department, and address the results in a current risk assessment.	Partially implemented. The Service Center issued a memorandum to the system owners in October 1997 outlining the alternatives identified in the feasibility study referenced in Recommendation G. 1. System owners responded in December 1997, agreeing to reduce the expiration period for passwords from 180 days to 90 days, reduce the allowable period of inactivity of a user ID from 180 days to 90 days, and remove inactive user IDs from the system after 1 year of inactivity. With the exception of one client, all inactive users are removed manually once a month. Procedures for removing Social Security inactive users are being developed.
H. 1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.	Implemented. Evaluation has been completed. This authority has been limited to three senior-level system programmers who work in the System Software Management Branch.

Recommendations	Status of Recommendations and Corrective Actions
H.2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical datasets maintained on the mainframe computers and to therefore provide an audit trail of system activity.	Implemented. Batch and TSO type 60 records are written to the SMF log. Type 60 record collection has been activated for "started tasks" as well.
I. 1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.	Implemented. Evaluation has been completed. Assignment of the OPERATIONS attribute has been restricted to employees who need the attribute to perform their duties.
1.2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.	Implemented. The feature OPERAUDIT has been activated, and the resultant logs will be reviewed on a quarterly basis by the Service Center Computer Security Manager.
J. 1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized.	Partially implemented. The identification of critical datasets has been completed, and a requirement to perform periodic reviews of reports auditing the critical datasets has been established. Performance of these actions would enable monitoring personnel to identify user access levels; however, the actions would not ensure that the user access level was authorized. Therefore, procedures need to be established to compare the critical dataset reports with approved user authorization requests.

Recommendations	Status of Recommendations and Corrective Actions
5.2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.	Implemented. A policy of "least privileged" access is in place.
K. 1. Evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF.	Implemented. The ADP Services Division has completed the evaluation and has identified adequate staffing within the Division for accomplishing the separation of the security administration and auditing functions. The security administration function will be maintained with the same staffing levels. The security auditing function will be placed within a quality management function in the Division's IRM and Customer Service Branch.
L. 1. Document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.	Implemented. While the Bureau disagreed with the recornrnendation, it has taken action to modify existing policy and procedures to reflect a new process.
M. 1. Provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Circular A- 130, Appendix III.	Implemented. A computer security plan for 1997 was developed and submitted to the Department of the Interior's Office of Information Resources Management.
N. 1. Perform a risk analysis of the Service Center's computer center and its applications.	Implemented. A risk analysis of the computer center has been completed.

Recommendations	Status of Recommendations and Corrective Actions

United States Department of the Interior

BUREAU OF RECLAMATION
Washington, D.C. 20240

IN REPLY REFER TO
D-5010
ADM-8.00

JUN 17 1998

Memorandum

To: Office of Inspector General
Attention: Robert J. Williams, Acting Inspector General

From: Eluid L. Martinez
Commissioner

Subject: Draft Audit Report on Followup of Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation (Assignment No. A-IN-BOR-00 l-97)

As required by Departmental Manual 360 DM 5.3, attached is the Bureau of Reclamation's written response to the subject audit report of our mainframe computer operations at the Denver Administrative Service Center (ASC). The schedule proposed for implementation of some of the recommendations recognizes the ASC's existing commitment to the complete implementation of the Federal Personnel Payroll System (FPPS) by the end of calendar year 1998.

While we generally support the audit recommendations, some of the discussion in the report is misleading and should be clarified. The report language regarding the FPPS system did not adequately consider that FPPS was under development during the time of the audit. According to the draft report, the period of audit coverage was fiscal year 1997. The FPPS was still in a development mode at that time, and there is a considerable difference between a software project in the development mode versus the maintenance mode. Some of the report language (e.g., page 10 of the draft report) could lead a reader to believe that FPPS is presently an unstable system. This is not true and should be clarified before the report is issued in final form.

We appreciate the opportunity to comment on the audit recommendations and anticipate working with your office towards a constructive resolution. If you have any questions or concerns, please contact Stan DUM, Administrative Service Center Director, at (303) 969-7200.

Attachment

cc. Assistant Secretary - Water and Science, Attention: Carla Burzyk
(w/ attachment)

OIG Draft Report "Followup of Mainframe Computer Policies and Procedures, Administrative Service Center"

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearance-s

Condition: In our prior report, we recommended that Service Center management require all contractor employees to have proper background clearances. However, during our current audit, we found that contractor personnel at the ADP Services Division had received background clearances but that not all contractor personnel at the FPPS and Financial Systems Divisions had received background clearances. Additionally, Service Center Federal personnel involved in designing, developing, operating, or maintaining sensitive automated systems did not have background checks and security clearances commensurate with their job responsibilities and the sensitivity of the information accessed. Specifically, 154 of the 189 Service Center employees who performed these ADP-related duties did not have the appropriate ADP background clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires agencies to establish and manage security policies, standards, and procedures that include requirements for screening individuals participating in the design, development, operation, or maintenance of sensitive applications or those having access to sensitive data. In addition' the Departmental Manual (441 DM 4.6) requires position sensitivity levels of "non-critical sensitive" or "critical sensitive" and associated security clearances for ADP-related positions for which employees are required to design, test, operate, and maintain sensitive computer systems. Security clearances are also required of employees who have access to or process sensitive data requiring protection under the Privacy Act of 1974. Further, the Departmental Manual (441 DM 5.15) requires that all consultants or contractors performing ADP-related sensitive and critical duties have background investigations to determine position suitability and to receive a security clearance.

Cause: Service Center management had not uniformly developed and implemented, across all Service Center Divisions, personnel security policies requiring contractor personnel who perform ADP-related sensitive and critical duties to be screened for position suitability. Additionally, Service Center management did not ensure that the level of position sensitivity for ADP-related positions was assigned at the level commensurate with the risk and sensitivity of the data accessed and processed and that background checks were performed on employees who filled these positions.

Effect: Without proper personnel background investigations, managers had limited knowledge of the suitability of their employees and contractors, from a security standpoint, for their respective jobs. Without this assurance, there was an increased risk that the Service Center's sensitive systems could be impaired or compromised by personnel.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Develop and implement policies and procedures which require contractor employees who fill ADP-related sensitive or critical positions to have documented suitability screening and proper background investigations and appropriate security clearances.

Response

Concur. The Denver Administrative Service Center (ASC) will develop and distribute policy to all affected ASC offices regarding security clearances and background investigations for contractor personnel. The policy will be distributed by October 1, 1998. In addition, the ASC will review and amend as necessary all personnel contracts to include the requirement for background investigations and security clearances for existing and future contract personnel by January 1, 1999. The responsible official is the Chief, Applications Management Office.

There are two types of contractual service arrangements at the ASC. Some employees work under a third-party contract with other agencies, usually the General Services Administration (GSA). In these cases, the servicing agency contract controls all contractual requirements and clauses. The requesting agency (ASC) may outline additional security requirements in the task order statement of work as long as the additional requirements are within the parameters of the original contract. All GSA contractors in both the ADP Services and Financial Systems Division were subject to background security investigations through GSA's requirements and procedures. These investigations were completed as of May 1997. As of March 1998, the Federal Personnel Payroll System (FPPS) Program Management Division contractor employees changed from a Department of the Army contract to a GSA contract. As a result of the preliminary audit findings, ASC security requirements were added to the task order under the GSA contract.

Another type of contractual arrangement is a direct contract between the ASC and the service contractor. All current direct contracts either already have the proper security clauses or will have the proper clauses by January 1, 1999, to comply with security requirements. All existing and future contractual service agreements will be reviewed to ensure compliance with the requirements for background security checks.

2. Evaluate the position sensitivity of ADP-related positions, assign position sensitivity levels in accordance with the Departmental Manual, and ensure that those employees working on sensitive systems have the proper background investigations and security clearances before they are assigned to the positions.

Response

Concur. The ASC will review ADP-related positions in the ASC organizations to verify the appropriate requirements for background investigations and security clearances, as required by the Departmental Manual to ensure employees working on sensitive systems have the proper background and security clearances. A complete evaluation of position sensitivities ASC-wide and the assignment of sensitivity levels will be completed by April 1, 1999. However, the ASC has no control over when the background investigations on these employees will be completed. These investigations are performed by an outside contractor. We believe that the contractor can complete most of these investigations by October 1, 1999. The responsible official is the Chief, Applications Management Office.

Position sensitivity evaluations for the ADP Services Division have been completed and the results of several background investigations received. The ASC began position sensitivity evaluations in the FPPS Division in June of 1998 with background investigations to follow. Position sensitivity evaluations for the Financial Systems Division (FSD) and PAY/PERS Division will commence after management decisions are made regarding potential reorganizations impacting the positions in these divisions.

While the ASC can control the position sensitivity evaluation process, it cannot control the timeframes in which the background investigations and security clearances are completed. The audit recommendation states that the background investigations and security clearances should be completed before the individuals are assigned to the positions. Our understanding is that this criteria only applies to positions classified as "Sensitive" (of which ASC has had very few thus far). Therefore, our concurrence is based on the understanding that employees currently occupying positions classified as "Non-Sensitive" may continue in those positions until such time as completed background investigations either confirm or rebut the appropriateness of their placement in these jobs.

B. Operating Efficiencies

Condition: At the Service Center, each division controlled the process of moving changed software from the test to the production environment, different software tools were used to control the movement of the changed software, and internal and external clients controlled their mainframe computer production scheduling.

Criteria: Office of Management and Budget Circular A- 130 states that management should oversee its processes to maximize return on investment and minimize financial and operational risk. Further, the Circular requires that financial management systems conform to the requirements of Office of Management and Budget Circular A-127, "Financial Management Systems. " Circular A- 127 requires that agency financial management systems process financial events effectively and efficiently.

Cause: Service Center management did not ensure that its processes were operating efficiently because of preferences of internal and external clients and because management had not developed and implemented consistent standards for controlling operational processes.

Effect: There was an increased risk that changed software would negatively impact the mainframe computer operating system; costs of maintaining different software tools would increase Service Center operating costs, which would be passed onto clients; and mainframe computer usage could be reduced. Additionally, without centralized control of production scheduling, there was an increased risk that critical processing jobs would not receive the required priority.

Recommendation:

We recommend that the Director, Administrative Service Center, in coordination with the Service Center's internal and external clients, evaluate the feasibility of centralizing the process of moving changed software from the test environment to the production environment, using standardized software tools to control the software change process, and centralizing mainframe computer production scheduling.

Response

Concur. The ASC will in coordination with internal and external clients perform an evaluation of the feasibility of centralized software change management. The feasibility analysis will include evaluating the viability of a standard software change management tool and make recommendations to management by October 1, 1999. In addition to evaluating centralized software change management, the ASC will also evaluate the feasibility of centralized computer production scheduling. Should the feasibility evaluation indicate that centralized change management and production scheduling is cost beneficial,

additional implementation time beyond the October 1, 1999, date will be necessary. The responsible official is the Chief, Applications Management Office.

There are several issues which this feasibility evaluation will need to consider. Due to the variety of customers ASC serves, centralized software change management will require technical expertise in a variety of different customer practices and utilities. Software change management is no longer simply a Common Business Oriented Language (COBOL) exercise. Without even considering the software change management tools our customers are using, there are multiple change management software tools even within the ASC. ChangeMan is the selected ASC change management software product that controls day-to-day changes on the IBM computer. This product is in various phases of implementation throughout the ASC. However, ChangeMan will not work within the COM-PLETE/Natural environment which FPPS uses. The PAC change management software tool was selected for this environment, due to the uniqueness of the Natural language. Since the intent of this recommendation appears to address the overall efficiency of mainframe computer operations, the intent of the feasibility evaluation will address this same concern as well.

SOFTWARE CHANGE MANAGEMENT

C. Application Software Change Management Controls

Condition: Software changes made to the FPPS during the latter stages of development and the early stages of implementation were not approved, reviewed, or evaluated adequately before changed software was installed for use in production; documentation was not adequate to monitor changes made to the software; and available library control software' was not implemented to ensure consistency and completeness throughout the FPPS application.

Criteria: Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," provides guidelines for managing software maintenance. Publication 106 states that all software changes should be carefully evaluated and formally reviewed prior to installing the changed software. The publication further states, "In order to monitor maintenance effectively, all activities must be documented. ... The key to successful documentation is that not only must the necessary information be recorded, it must be easily and quickly retrievable by the maintainer." In addition, FPPS Division policies and procedures require that all changes to the FPPS application be thoroughly documented, be accepted by all involved parties, and pass a quality assurance review.

Cause: FPPS Division management did not ensure that Division personnel followed software change management practices for making software changes to the FPPS application because of the time constraints to implement FPPS and because FPPS was encountering problems and was considered by Division personnel to be unstable. In addition, we found that FPPS Division management did not hold its personnel accountable for complying with Division policies and procedures when they made changes to the FPPS application. Further, FPPS Division management said that they did not implement the available library control software, which would ensure adequate documentation of the FPPS application, because at that time, the vendor library control software was not working correctly.

Effect: There was an increased risk that the changes made to the FPPS application would not perform according to specifications, which could adversely affect user satisfaction and could adversely impact other applications interfacing with the FPPS application or the mainframe operating system.

Recommendations:

We recommend that the Director, Administrative Service Center:

'Library control software is a system for keeping track of changes to and versions of software programs, documenting components to build executable programs, and preventing unauthorized access to program files.

1. Require that software changes be adequately reviewed and approved before the changes are implemented.

Response

Complied. Currently, FPPS Standard Operating Procedures (SOP) require that any software changes complete the following steps:

- Be approved by FPPS management before programming begins.
- Be migrated to a dedicated test environment upon completion with an explanation of the change(s) made.
- Be independently tested and approved for production by FPPS Functional Analysts and have the test results and documentation reviewed and approved by an FPPS Functional Lead.
- Be independently migrated to production by the FPPS Database Administrative staff along with any database changes required.

This SOP is enforced by FPPS Management.

2. Implement procedures to ensure that all software changes to the FPPS application are properly documented.

Response

Complied. The FPPS SOP requires that any software changes be fully documented on the change request form or problem report form. It also requires that any change (s) made be fully documented on the migration request forms and that a responsible person's signature be provided at each step along the way. Upon migration to production, all paperwork is filed for easy retrieval.

This SOP is enforced by FPPS Management.

3. Implement the available library control software when corrected to ensure adequate documentation of the FPPS application.

Response

Concur. The available library control software is in the process of being implemented for testing. Once it is to the stage that it will meet all our migration needs and is fully tested,

it will be implemented. The target date to debug, test, and render a "go or no-go" decision on implementation of available library control software is July 1, 1999. The responsible official is the Chief, Applications Management Office.
The FPPS SOP does provide adequate documentation and an organized systematic migration approach which also provides separation of duties. This SOP can also be used for emergency change reports which are a fact of life for any new system. One of the

reasons the library control software is not used is that it does not provide emergency change flexibility as our current SOP does. As FPPS completes the transition from a development mode to a maintenance mode, the computer operating environment will almost certainly change substantially. It will take time to determine how interrelated conditions will develop so as to determine specifically what corrections are needed to make the library control software operational.

SOFTWARE CHANGE MANAGEMENT

D. Operating System Software Change Management

Condition: Change controls over the mainframe computer operating system software were not adequate. The ADP Services Division change control procedures did not address adequate separation of duties between the development, test, and installation functions. Thus, one individual could perform all of these critical functions. In addition, the change control procedures did not ensure that all changes were properly approved by Division management. While the change management procedures required approval of all software changes, changes were made without documented evidence of approval.

Criteria: Appendix III of Office of Management and Budget Circular A- 130 states that one of the minimum controls required in a general support system is personnel controls. One such control is separation of duties, which is "the practice of dividing the steps in a critical function among different individuals." Also, Federal Information Processing Standards Publication 106 states that "to be effective, the policy should be consistently applied and must be supported and promulgated by upper management to the extent that it establishes an organizational commitment to software maintenance. " In addition, Publication 106 states that "prior to installation, each change (correction, update, or enhancement) to a system should be formally reviewed." Finally, Division system change request procedures require that all change requests be approved by the appropriate branch chief

Cause: ADP Services Division management did not ensure that appropriate separation of duties existed in developing and testing mainframe operating system software and parameter changes and in moving operating system software and parameter changes into the production environment, although the number of employees within the Division may allow for a separation of these duties. Additionally, Division management had not implemented controls to ensure that the process of making system software changes was in compliance with its documented procedures. Further, management had not implemented procedures to require periodic reviews of critical datasets and system parameters to identify inappropriate changes to the mainframe operating system environment. Although Division management had implemented a change control software tool that provided a systematic and automated means of controlling the movement of software changes, all the capabilities of the software tool were not implemented because of other Division priorities.

Effect: There was an increased risk that unauthorized, untested, and undocumented changes could be made to the mainframe computer operating system software and parameters, which would affect system processing and data integrity, and that these changes would not be detected or detected in a timely manner.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate current ADP Services Division procedures and determine the feasibility of implementing controls in the change management process over operating system software to ensure that adequate separation of duties is addressed and complied with.

2. Develop procedures and implement controls to ensure that changes to the operating system parameters are identified, approved by ADP Services Division management, and documented.

3. Develop procedures requiring periodic reviews of critical datasets and system parameters.

4. Evaluate implementing available capabilities in the current change control software tool to more effectively control changes to the operating system software.

Response

Concur. The ASC will implement the recommended actions by July 1, 1999. The responsible official is the Chief, ADP Services Division.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

E. System Audit Tools

Condition: Service Center management did not use available mainframe computer operating system audit tools that would improve integrity over system processing and data and that would detect inappropriate actions by authorized users. Specifically:

- Operating system integrity verification and audit software was not used. Such software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures that may result from system setting options; from installing "back doors" to the operating system; and from introducing viruses and Trojan horses, which can destroy production dependability and circumvent existing security measures.

- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. System options that would log the results in the SYSLOG[2] of actions taken by the computer operators and system programmers affecting mainframe operating system configuration were not implemented. Therefore, an audit trail of the system initialization process and changes to the operating system configuration could not be produced for periodic review. Based on recommendations made by our audit staff during the review, Service Center management implemented the logging capabilities within the system; however, procedures had not been developed and implemented to require periodic reviews of the logs.

- Periodic reviews of critical System Management Facility (SMF)[3] logs to identify unauthorized changes to data by authorized users and critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as SET TIME, SET DATE, and SET SMF, all of which affect system processing and audit trails.

Criteria: Appendix III of Office of Management and Budget Circular A-130 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability includes reviewing or looking at

[2]SYSLOG is an audit trail that logs the results of actions taken by computer operators and system programmers during system initialization.

[3]The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identifying users who performed the activity.

patterns of users' behavior, which requires periodic reviews of the audit trails. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that audit trails are "technical mechanisms" to achieve individual accountability.

Cause: **Service** Center management did not acquire operating system integrity and verification software, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of available system logs. Instead, Service Center management relied on its staff to make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect: **As** a result, there was an increased risk that mainframe computer operating system security exposures would not be identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or detected timely and that the responsible individuals would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate acquiring system verification and auditing software.

Response

Concur. The ASC will develop functional requirements and identify additional resources necessary to manage and conduct evaluation of existing verification and auditing products to determine cost and capability. Should a software product be found which complies with our requirements, it will be implemented by January **1,** 1999. The responsible official is the Chief, ADP Services Division.

2. Develop and implement procedures to ensure that periodic reviews are performed of the SYSLOG and critical SMF logs to identify unauthorized or inappropriate activities and that unauthorized or inappropriate activities are reported to Service Center management.

Response

Concur. The ASC will develop and implement procedures for reviewing SYSLOG and critical SMF logs by July 1, 1999. The responsible official is the Chief, ADP Services Division.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

F. Mainframe Operating System Options

Condition: ADP Services Division management did not implement mainframe operating system options that would strengthen controls over computer programs which access sensitive operating system functions. We found 13 libraries[4] that were able to run in the "Authorized Program Facility (APF)-authorized" state, even though the libraries were not required to run in the APF. By running in the APF-authorized state, these libraries may be considered part of the mainframe operating system and thus have access to all of the mainframe resources.

Criteria: IBM's publication titled "OS/390 Initialization and Tuning Reference" states that "the parameter **LNKAUTH** specifies whether all libraries" in the **LNKLST**** member[5] "are to be treated as Authorized Program Facility (APF)-authorized when accessed as part of the concatenation, or whether only those libraries that are named in the APF table are to be treated as APF-authorized."[6] Additionally, the publication addresses managing system security and states that the "authorized program facility (APF) allows your installation to identify system or user programs that can use sensitive system functions. "

Cause: Division Management implemented a default option (LNKLST) that allowed libraries within the **LNKLST**** member to run in the APF-authorized state. An alternative option (APFTAB) is provided which requires only those libraries that are named specifically in the APF table to be able to run in the APF-authorized state. The 13 libraries were automatically added to the **LNKLST**** member when the operating system was upgraded in July 1997. Because Division management did not review the members used to define APF-authorized libraries, these 13 libraries remained in the **LNKLST**** member. Further, because Division management implemented the LNKLST option, these 13 libraries were unnecessarily provided the ability to run in the APF-authorized state. Therefore, management did not have assurance that only approved libraries had access to sensitive operating system functions. Based on recommendations of our audit staff' during the review, the

---

[4] A library is a collection of programs or data files or a collection of functions (subroutines) that are linked into the main program when it is compiled. (The Computer Language Company, Inc., Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

[5] Concatenation means to link together in a series or chain. ('Webster's Ninth New Collegiate Dictionary, Merriam-Webster Inc., Springfield, Massachusetts, 1989, p. 27 1.)

[6] **LNKLST**** member "defines the collection of program libraries to be searched, in sequence, for programs when no specific [library] has been supplied in the job stream." (Mark S. Hahn CONSUL Risk Management, Inc., A Guide to SYS1.PARMLIB, Monograph Series 4, The Information Systems Audit and Control Foundation, Inc., Rolling Meadows, Illinois, February 1996, p. 38.)

libraries were removed from the LNKLST** member. However, if the APFTAB option had been used, Division personnel would have been required to enter the 13 library names into the APF table, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Effect: By implementing the LNKLST option rather than the APFTAB option, the risk increased for unauthorized libraries to run in an authorized state, thus bypassing operating system controls, and for system integrity to be lost.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate the feasibility of using the APFTAB option, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Response

Concur. The ASC will review the existing control methodology and determine if using the APFTAB option would provide enough additional safeguards to justify its implementation. The review will be completed and recommendations provided to management by July 1, 1998. The responsible official is the Chief, ADP Services Division.

2. Perform periodic reviews of all members used to define the APF-authorized libraries to ensure that only those required to run in the APF-authorized state are given this authority.

Response

Concur. The ASC will by October 1, 1998, develop procedures requiring periodic reviews of members used to define the APF-authorized libraries. The responsible official is the Chief, ADP Services Division.

STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
C.l and C.2	Implemented.	No further action is required.
A.l, A.2, B.1, C.3, D.l, D.2, D.3, D.4, E.l, E.2, F.l, and F.2	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.l, B.l, C.1, D.l, D.2, E.l, F.l, F.2, F.3, G.l, H.l, H.2, I.1, I.2, J.2, K.1, L.l, M.l, N.l, N.2, and 0.1	Implemented.	No further action is required.
D.3, G.2, and J.l	Resolved; not implemented.	No further response to the Office of Inspector General is required. The information regarding the status of these recommendations will be provided to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
Mail Stop 5341
Washington, D. C . 20240

Our 24-hour
Telephone HOTLINE
l-800-424-508 1 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420 or
l-800-354-0996

Outside the Continental United States

Caribbean Region

U. S . Department of the Interior
Office of Inspector General
Eastern Division - Investigations
4040 Fairfax Drive
Suite 303
Arlington, Virginia 22201

(703) 235-922 1

North Pacific Region

U.S. Department of the Interior
Office of Inspector General
North Pacific Region
415 Chalan San Antonio
Baltej Pavilion, Suite 306
Tamuning, Guam 96911

(67 1) **647-605** 1

Toll Free Numbers:
l-800-424-508 1
T'DD l-800-354-0996

FTS/Commercial Numbers:
(202) 208-5300
TDD **(202) 208-2420**

HOTLINE

1849 C Street' N.W.
Mail Stop 5341
Washington, D.C. 20240